МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

«**ЗАТВЕРДЖУЮ**»
Завідувач кафедри
д.т.н., проф. Рудницький В.М.
_____
«_____» _____ 20___ р.

РОБОЧА ПРОГРАМА
навчальної дисципліни

«КРИПТОГРАФІЧНІ МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

підготовки здобувачів освітнього ступеня «бакалавр»

напряму підготовки – 6.170103 «Управління інформаційною безпекою»

2016 – 2017 н.р.

Робоча програма навчальної дисципліни «Криптографічні методи та засоби захисту інформації» підготовки здобувачів освітнього ступеня «бакалавр» за напрямом підготовки 6.170103 «Управління інформаційною безпекою» 9 стор.

Робоча програма складена на основі програми навчальної дисципліни «Криптографічні методи та засоби захисту інформації», шифр (за ОПП) – ВФП9.

Розробник програми: Стабецька Тетяна Анатоліївна, асистент кафедри інформаційної безпеки та комп'ютерної інженерії

Робоча програма затверджена на засіданні кафедри інформаційної безпеки та комп’ютерної інженерії.

Протокол № ___ від “____”_____20__ року

© _____, 20__ рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів –4</td><td><u>Галузь знань</u>
1701«Інформаційна безпека»</td><td>вибіркова</td></tr>
<tr><td rowspan="4">Загальна кількість годин -120</td><td rowspan="4"><u>Напрям підготовки</u>
6.170103 «Управління інформаційною безпекою»</td><td>Рік підготовки:</td></tr>
<tr><td>2</td></tr>
<tr><td>Семестр</td></tr>
<tr><td>3</td></tr>
<tr><td rowspan="8">Змістових модулів – 2</td><td rowspan="8"><u>Рівень вищої освіти</u>
перший (бакалаврський)</td><td>Лекції</td></tr>
<tr><td>16 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>32 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>72 год.</td></tr>
<tr><td>Залік в кінці 3-го семестру.</td></tr>
</table>

Примітка:

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми навчання – 60%.

Мета викладання навчальної дисципліни полягає у формуванні у майбутніх фахівців сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення криптографічного захисту інформації в комп'ютерних системах, формуванні у студентів розуміння основ інформаційної безпеки, вмінню застосовувати криптографічні методи шифрування, використовувати методи шифрування інформації для передачі у мережі, а також надання студентам системних знань з принципів побудови систем криптографічного захисту інформації в КС.

Завданнями вивчення навчальної дисципліни є:

- оволодіння теоретичними знаннями про основні методи криптографічного захисту інформації;
- розгляд математичних моделей симетричних шифрів та їх властивостей;
- оволодіння основними способами шифрування даних;

- вивчення методів асиметричної криптографії;
- дослідження особливостей криптографічних алгоритмів та криптографічних протоколів;
- розгляд основних напрямків розвитку сучасних систем КЗІ.

3. Компетенції, що формуються після опанування дисципліни:

- обґрунтування та висування пропозицій щодо стандартних криптографічних систем, криптографічних примітивів та протоколів захисту ресурсів в КС та КМ;
- здійснення загальної оцінки якості криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що реалізовані з використанням засобів обчислювальної техніки.

4. Тематичний план дисципліни

Змістовий модуль 1. «Основні поняття криптографії. Криптографія з симетричним ключем»

Тема 1.1. *Базові поняття криптографії.*

Мета і задачі дисципліни. Основні поняття та визначення. Наука про шифрування. Роль криптографії у захисті даних.

Тема 1.2. *Історія кодування та шифрування. Використання кодів. Сучасна криптографія.*

Історія криптографії. Основні поняття криптографії та теорії секретних систем. Перші методи шифрування перестановки та заміни. Одноалфавітні системи шифрування Віженера, Плейфейра та інш. Багато алфавітні системи шифрування та їх роль у сучасній криптографії.

Тема 1.3. *Прості шифри перестановки. Криптоаналіз шифрів перестановки.*

Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка. Прості шифри. Криптоаналітичні атаки та метод підрахунку частот для моно та багатоалфавітних криптосистем.

Тема 1.4. *Шифри простої та складної заміни.*

Тема 1.5. *Багатоалфавітні шифри.*

Числові шифри. Книжкові шифри.

Тема 1.6. *Симетричні алгоритми.*

Блочні та поточні шифри. Принципи побудови, функціонування та криптоаналізу симетричних блокових алгоритмів шифрування DES (Digital Encryption Standard), ГОСТ 28147-89, AES.

Тема 1.7. *Шифрування із паролем.*

Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.

Змістовий модуль №2. «Розподіл ключів та криптографія з відкритим ключем»

Тема 2.1. *Розподіл ключів. Використання довіреної третьої сторони.*

Тема 2.2. *Криптографія з відкритим ключем та цифрові конверти.*

Алгоритм RSA. Алгоритм Діффі (DH). Алгоритм на основі задачі про укладку ранця. Алгоритм еліптичних кривих. Порівняння алгоритмів.

Тема 2.3. *Цифровий підпис.*

Алгоритми цифрового підпису. Порівняння алгоритмів.

Тема 2.4. *Нормативно-правове регулювання у галузі КЗІ* .

Державне регулювання господарських відносин у сфері криптографічного захисту інформації в Україні. Правове регулювання ЕЦП в Україні та світі. Державний контроль та право суспільства на криптографію. Міжнародні стандарти в сфері КЗІ. Стандартизація в сфері КЗІ в Україні

Тема 2.5. *Основні напрямки розвитку сучасної криптографії*

Шифрування на еліптичних кривих. Методи диференціального криптоаналізу. Квантова криптографія.

5. Структура навчальної дисципліни

Назви тем	***Кількість годин***				
	денна форма				
	Усього	у тому числі			
		Лекції	**Прак. роботи**	**Лаб. роботи**	**Сам. робота**
Змістовий модуль 1. «Основні поняття криптографії. Криптографія з симетричним ключем»					
Тема 1. Базові поняття криптографії.	***4***	2			2
Тема 2. Історія кодування та шифрування. Використання кодів. Сучасна криптографія.	***10***	2		2	6

Тема 3. Прості шифри перестановки. Криптоаналіз шифрів перестановки.	***10***	2		2	6
Тема 4. Шифри простої та складної заміни.	***12***	2		4	6
Тема 5. Багатоалфавітні шифри.	***8***			2	6
Тема 6. Симетричні алгоритми.	***10***	2		4	4
Тема 7. Шифрування із паролем.	***8***			2	6
Разом за модулем	***62***	*10*		*16*	*36*
Змістовий модуль №2. «Розподіл ключів та криптографія з відкритим ключем»					
Тема 1. Розподіл ключів. Використання довіреної третьої сторони.	***10***	2		2	6
Тема 2. Криптографія з відкритим ключем та цифрові конверти.	***12***			4	8
Тема 3. Цифровий підпис.	***14***	2		4	8
Тема 4. Нормативно-правове регулювання у галузі КЗІ .	***14***	2		4	8
Тема 5. Основні напрямки розвитку сучасної криптографії	***8***			2	6
Разом за модулем	***58***	*6*		*16*	*36*
Усього годин	**120**	**16**		**32**	**72**

6.Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Історія кодування та шифрування. Використання кодів. Сучасна криптографія.	2
2	Прості шифри перестановки. Криптоаналіз шифрів перестановки.	4
3	Шифри простої та складної заміни.	4
4	Багатоалфавітні шифри.	2
5	Симетричні алгоритми.	6

6	Шифрування із паролем.	2
7	Розподіл ключів. Використання довіреної третьої сторони.	2
8	Криптографія з відкритим ключем та цифрові конверти.	4
9	Цифровий підпис.	4
10	Нормативно-правове регулювання у галузі КЗІ .	4
11	Основні напрямки розвитку сучасної криптографії	2
	Разом:	***32***

7. Теми для самостійної роботи

№ п/п	**Назва теми**	**Кількість годин**
1	Базові поняття криптографії.	2
2	Історія кодування та шифрування. Використання кодів. Сучасна криптографія.	2
3	Прості шифри перестановки. Криптоаналіз шифрів перестановки.	2
4	Шифри простої та складної заміни.	8
5	Багатоалфавітні шифри.	10
6	Симетричні алгоритми.	8
7	Шифрування із паролем.	8
8	Розподіл ключів. Використання довіреної третьої сторони.	10
9	Криптографія з відкритим ключем та цифрові конверти.	10
10	Цифровий підпис.	8
11	Нормативно-правове регулювання у галузі КЗІ .	2
12	Основні напрямки розвитку сучасної криптографії	2
Всього:		***72***

8. Перелік індивідуальних навчально-дослідних завдань

1. Сучасні симетричні криптосистеми. Американський стандарт шифрування даних DES. Основні режими роботи. Режим "Електронна кодова книга". Режим "Зчеплення блоків шифру". Режим "Зворотний зв'язок по шифру". Режим "Зворотний зв'язок по виходу". Області застосування алгоритму DES. Криптоаналіз.
2. Сучасні симетричні криптосистеми. Стандарт шифрування даних ГОСТ 28147-89. Режим простої заміни. Режим вибірки гами. Режим шифрування зі зворотним зв'язком. Режим вироблення імітовставки.
3. Сучасні симетричні криптосистеми. Потокові шифри. Генератори псевдовипадкових послідовностей.
4. Сучасні симетричні криптосистеми. Алгоритм RC-4. Опис криптосхеми. Криптоаналіз.
5. Сучасні асиметричні криптосистеми. Концепція криптосистеми з відкритим ключем. Односпрямовані функції. Криптосистема шифрування даних RSA. Процедури шифрування і розшифрування в криптосистемі RSA. Безпека і швидкодія криптосистеми RSA. Криптоаналіз.

9. Рекомендована література

Основна:

1. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.

2. Бернет С., Пэйн С., Криптография. Официальное руководство RSA Security. Изд. 2-е, стереотипное. – М.: ООО «Бином-Пресс», 2007. – 384 с.: ил.

3. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 256 с.

4. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.

5. Бабаш А. В. Криптография. – М.: СОЛОН-Пресс, 2007. – 511 с.

6. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии: Учебное пособие. М.: Горячая Линия - Телеком, 2002. – 175 с.

7. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. М.: Издательство: АНО НПО "Профессионал", 2005. – 480 с.

8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2001. – 480 с.

Додаткова:

1. Маховенко Е. Б. Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006. – 320 с.

2. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО Полиграф-Консалдинг, 2005. – 209 с.

3. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. М.: Горячая линия – Телеком, 2005. – 229 с.

4. Ростовцев А.Г. Алгебраические основы криптографии. М.: НПО «Мир и семья», ООО «Интерлайн», 2000. – 256 с.

5. Погорелова Б.А. Словарь криптографических терминов. М.: МЦНМО, 2006. – 94 с.

10. Інформаційне забезпечення

1. Журнал “Конфидент”, м. С.-Петербург (http://www.confident.ru)

2. Журнал “Захист інформації” м. Київ

3. Журнал “Безопасность и бизнес” м. Київ - (www.bsm.com.ua)

4. Журнал “Сучасна спеціальна техніка” м. Київ

5. http://www.pgpi.com – сайт розробника алгоритму і програми PGP

6. https://infocity.kiev.ua – Центр комп’ютерної безпеки, м. Київ

7. www.antivir.ru – ЗАТ “ДіалогНаука”, м. Москва (розробник DrWeb)

8. http://www.naiau.kiev.ua – сайт Національної академіїї внутрішніх справ

9. http://ci.uz.gov.ua/common/acts.html

11. Критерії оцінювання навчальних досягнень

Поточне тестування та самостійна робота студентів												**Сума**
Змістовий модуль №1							***Змістовий модуль № 2***					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т1	Т2	Т3	Т4	Т5	100
5	5	10	10	10	10	10	5	5	10	10	10	

Т1, Т2, …, Т5 – теми змістових модулів.